IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A method of providing transport-independent secure communications in a computer network, comprising the steps of:

directly receiving application data, from an application, at an upper connection layer of a transport protocol stack, wherein the application data is received from the application using a connection specific application programming interface (API) desired for communication by the application and which is not associated with security, ~~the application data directly received from an application~~;

passing the application data from the upper connection layer to a security layer from within the transport protocol stack and unbeknownst to the application;

encrypting the application data within the security layer;

passing the encrypted application data from the security layer to a lower connection layer of the transport protocol stack; and

sending the encrypted application data from the lower connection layer out a network connection;

wherein the application is not required to perform security handshakes in order to send encrypted application data over the network, the connection layers support at least one network transport protocol, and the security layer is not specific to that transport protocol.

2. (Original) The method of claim 1, further comprising the steps of receiving at the lower connection layer encrypted application data which came in at the network connection; passing the encrypted application data from the lower connection layer to the security layer; decrypting the application data within the security layer; passing the decrypted application data from the security layer to the upper connection layer; and sending the decrypted application data from the upper connection layer to the application, without requiring that the application perform a security handshake.

3. (Original) The method of claim 1, further comprising the step of the lower connection layer establishing a connection with a handshake mode that is at least one of an interactive mode and a blind-root-accept mode.

4. (Original) The method of claim 1, further comprising the step of the lower connection layer establishing a connection with a handshake mode that is at least one of a server mode, a client mode, and a server with client authentication enabled mode.

5. (Original) The method of claim 1, further comprising the step of changing a list of trusted roots for the secure connection.

6. (Original) The method of claim 1, further comprising the step of the security layer informing at least one of the connection layers of security handshake proceedings.

7. (Currently Amended) A system for secure computer networking, comprising:

an application which is free of code for performing security procedure handshakes for secure network communications;

at least one connection layer directly interfaced with the application, the connection layer comprising an upper connection layer associated with a transport protocol stack and a lower connection layer associated with the transport protocol stack, the connection layers comprising code for performing at least one network transport protocol; and

a security layer callable from the connection layer rather than the application and wherein the security layer is unbeknownst to the application, the security layer comprising code for performing security procedure handshakes for secure network communications, the security layer also comprising code for encrypting and decrypting application data, and wherein the application initially sends application data to the protocol stack of the upper connection layer directly using a desired application programming interface (API) associated with a connection mechanism that is not associated with security.

8. (Original) The system of claim 7, wherein the connection layers comprise code for performing a WinSock network transport protocol.

9. (Original) The system of claim 7, wherein the security layer comprises code for performing security procedure handshakes for a Secure Sockets Layer session.

10. (Original) The system of claim 7, wherein the security layer comprises code for performing security procedure handshakes for a Transport Layer Security session.

11. (Original) The system of claim 7, wherein the application comprises code for providing Lightweight Directory Access Protocol services.

12. (Original) The system of claim 7, comprising a means for the security layer and at least one of the connection layers to identify a particular application and its cryptographic properties.

13. (Original) The system of claim 7, comprising a means for the security layer and at least one of the connection layers to identify a function as a call back function.

14. (Original) The system of claim 7, comprising a means for establishing a secure connection using a specified handshake mode.

15. (Original) The system of claim 7, further comprising a legacy application which performs security handshakes, and a security module supporting a secure connection to the legacy application.

16. (Currently Amended) A configured storage medium embodying data and instructions readable by a computer to perform a method of processing application data for secure network communications, the method comprising the computer-implemented steps of:

at a security layer, receiving a request from a lower connection layer of a transport protocol stack to establish a secure connection, wherein an application that utilizes the security layer is unaware of the security layer and its operations;

in response, utilizing a means for establishing a connection to establish the requested connection; and

at the security layer, receiving encrypted application data from the lower connection layer, decrypting the application data, and passing the decrypted application data to an upper connection layer of the transport protocol stack;

whereby the application directly receives the decrypted application data without being required to perform security procedure handshakes for secure network communications and without being aware of security communications that occur via the security layer, and wherein the application receives the decrypted application data in a desired application programming interface (API) associated with a connection that the application originally used and that is not associated with security.

17. (Original) The configured storage medium of claim 16, wherein the means for establishing a connection establishes a Secure Sockets Layer connection.

18. (Original) The configured storage medium of claim 16, wherein the method further comprises receiving the encrypted application data at the lower connection layer using a transport model.

19. (Previously Presented) The configured storage medium of claim 18, wherein the lower connection layer uses a proxy transport model.

20. (Original) The configured storage medium of claim 16, further comprising a signal embodied in the computer, the signal comprising a secure network communications protocol stack interface which is callable from at least the lower connection layer.